

AUTOMATICKÁ BEZPEČNOST

Martin Sláma, Komix

V uplynulém roce jsme byli svědky rozšíření technologie webových služeb jako součásti intranetových, ale i internetových řešení. Obchodní příležitosti rychle tlačí do popředí zajištění bezpečnosti použití této technologie.

Webové služby představují technologii distribuovaného zpracování založenou na poskytnutí aplikačních služeb na internetu nebo intranetu na bázi standardu XML (eXchange Markup Language). XML dokument umožňuje přenášet všechny typy informací. To, co webová služba zvládá, se definuje pomocí rozhraní WSDL (Web Services Definitions Language). WSDL umožňuje specifikovat operace, se kterými daná služba pracuje. Kromě popisu obsahu definuje WSDL i to, kde je služba dostupná a jaký komunikační protokol je použit ke spojení s ní. Máme-li definovanou službu a příslušné operace, je možné k dané službě přistoupit.

Čím více budeme chtít aplikace zabezpečit, tím více strojového času bude třeba

SOAP středem všeho

K tomu využijeme protokol SOAP (Simple Object Request Protocol), pomocí kterého můžeme danou operaci vyvolat, předat jí požadované parametry a vrátit výstup. SOAP sám o sobě vystupuje jako obálka, která vše zabalí a dopraví na správné místo. Jako transportní protokol při tom může posloužit např. HTTP nebo SMTP. Aby bylo možné webové služby využít, je nutné dozvědět se o jejich existenci a rozhraní, které poskytují. K tomu slouží registr služeb, který je určitou obdobou Zlatých stránek. Tyto informace se ukládají a publikují prostřednictvím technologie UDDI (Universal Discovery and Description Integration).

Příklady použití

Klíčovou oblast rozhodující o masovém použití webových služeb představují jejich bezpečnostní standardy. Těžko si představit použití těchto služeb při obchodních transakcích typu bankovního příkazu či nákupu akcií, aniž by byly použity náležitě bezpečnostní mechanismy. Proces standardizace WS-Security (jak je specifikace označována), na kterém úzce spolupracují mimo jiné i IBM a Microsoft, významně pokročil, dosud však není dokončen.

Není-li zajištěna bezpečnost webových služeb, hrozí tato základní bezpečnostní rizika spadající do klasických oblastí zabezpečení:

» **Neautorizovaná transakce:** např. klient banky posílá zprávu SOAP požadující vyzvednutí peněz a transakce je neautorizovaná. Riziko řešíme použitím autentizačního mechanismu podle specifikace WS-Security. Příkladem je zahrnutí username/password do zprávy SOAP.

» **Zpráva SOAP je veřejně čitelná – bez kryptování,** a tím pádem je k dispozici narušiteli – může jít např. o číslo bankovního účtu a jeho stav. Řešením rizika je konvertování textu do nečitelné podoby zašifro-

váním, a to na úrovni transportní vrstvy (SSL), případně na úrovni vrstvy zpráv (WS-Security specifikace).

» **Zpráva SOAP je modifikovatelná – bez integrity.** Hrozí, že narušitel zprávu nelegálně modifikuje, např. změní číslo účtu. Narušení integrity zprávy lze opět řešit mechanismem popsáním ve specifikaci WS-Security.

Obecně platí, že čím více budeme chtít aplikace zabezpečit, tím více strojového času bude třeba. Bezpečnost webových služeb je zajišťována v transportní vrstvě (SSL) a ve vrstvě zpráv (WS-Security specifikace). Na jejich celkovém zabezpečení se však podílejí také další vrstvy.

Zatímco zabezpečení na úrovni transportní vrstvy zašifruje celou zprávu, WS-Security nabízí možnosti optimalizace zabezpečení (část zprávy), a tím snižuje nároky na procesor.

Specifikace WS-Security obsahuje standardní množinu rozšíření SOAP, která poskytují právě zajištění autentizace, důvěryhodnosti a integrity (označuje se jako WS-Security Language). Je otevřená k dalším bezpečnostním modelům jako PKI, Kerberos či SSL. Poskytuje podporu pro četné bezpečnostní tokeny, rozličné formáty digitálních podpisů, kryptovací technologie a důvěryhodné domény (trusted domains).

WS-Security autentizace

Autentizace brání odesilatelci se vydávat za někoho jiného. V zabezpečené zprávě je uvedeno username/password, tzv. *základní autentizace*. Webová služba je zpracována pouze, pokud je kombinace username/password platná. Alternativou je např. použití digitálního podpisu.

WS-Security integrita

Integrita chrání zprávu před neoprávněnou modifikací. Z klíče, který má k dispozici pouze odesilatel, vytváří za použití určeného algoritmu digitální podpis XML na základě obsahu části zprávy (v úvahu připadají její *tělo*, *security token*, *timestamp*). Pokud dojde ke změně zprávy, není již kompatibilní s digitálním podpisem XML. Příjemce rovněž vytvoří z obdržené zprávy podpis. Jsou-li podpisy různé, je odesilatel zasláno hlášení o chybě, aniž by došlo ke zpracování zprávy příjemcem.

WS-Security důvěryhodnost

Důvěryhodnost chrání obsah zprávy před čtením neautorizovaným příjemcem. Povoleno je kryptování částí zprávy *těla*, *hlavičky* a *přílohy*. Ke kryptování je třeba klíče a algoritmu.

SOAP/HTTP transport channel security

Tento způsob zabezpečení předcházelo použití WS-Security. Využívá protokolu HTTPS a zabezpečuje, na rozdíl od selektivního rozsahu kryptování ve vrstvě zpráv WS-Security, celý datový paket HTTP. Jednou z nevýhod je, že ke zjištění informace o směrování je třeba celou zprávu dešifrovat.

Rozšíření WS-Security

Protože standard WS-Security řeší jen část bezpečnostních služeb – nepracuje např. s auditem, garancí neodmítnutelnosti apod. – připravuje se pro webové služby za účasti firem IBM či Microsoft komplexní řešení, tzv. *security model framework*.

Standard WS-Security nalézá uplatnění na internetu. Jako perspektivní se jeví především oblast státní správy, kde i u nás probíhají první kroky s využitím webových služeb (např. sdílení registrů a dalších informací spravovaných orgány státní správy). Následovat samozřejmě budou i komerční oblasti a finančníctví. □